2

Governança Corporativa e Regulamentações de *Compliance*

Como vimos no início deste livro, a TI deve atender às necessidades do negócio e também a marcos de regulação externos.

Em organizações que apresentam um grau de Governança Corporativa mais avançada, a Governança de TI tem grande interação com sistemas de controle interno e de gestão de riscos corporativos.

Dependendo do negócio, existem vários marcos reguladores. Por exemplo, uma empresa de telecomunicações no Brasil deve atender a uma série de instrumentos regulatórios provenientes da Anatel. O mesmo ocorre com os bancos, em relação às normas do Banco Central ou com as organizações que possuem ações na BMF-Bovespa, em relação às normas da Comissão de Valores Mobiliários.

De qualquer forma, essas regulamentações geralmente são transformadas em objetivos e entidades de controle no contexto da Governança Corporativa.

2.1 Governança Corporativa e a ligação com a Governança de TI

De acordo com o Instituto Brasileiro de Governança Corporativa – IBGC (2009), a Governança Corporativa consiste:

> *no sistema pelo qual as sociedades são dirigidas, monitoradas e incentivadas, envolvendo o relacionamento entre proprietários, Conselho de Administração, Diretoria e órgãos de controle interno. As boas práticas de governança corporativa convertem princípios em recomendações objetivas alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade.*

Os princípios da Governança Corporativa, ainda de acordo com IBGC (2009), são:

- **Transparência:** obrigação e desejo de informar resultados e ações.
- **Equidade:** tratamento igual para todos os acionistas.
- **Prestação de contas:** os agentes da governança corporativa prestam contas e são responsáveis pelos seus atos e omissões.
- **Responsabilidade corporativa:** os agentes de governança devem zelar pela sustentabilidade das organizações, visando a sua longevidade, incorporando considerações de ordem social e ambiental na definição dos negócios e operações.

A Figura 2.1 apresenta, de acordo com o IBGC, o Sistema de Governança Corporativa.
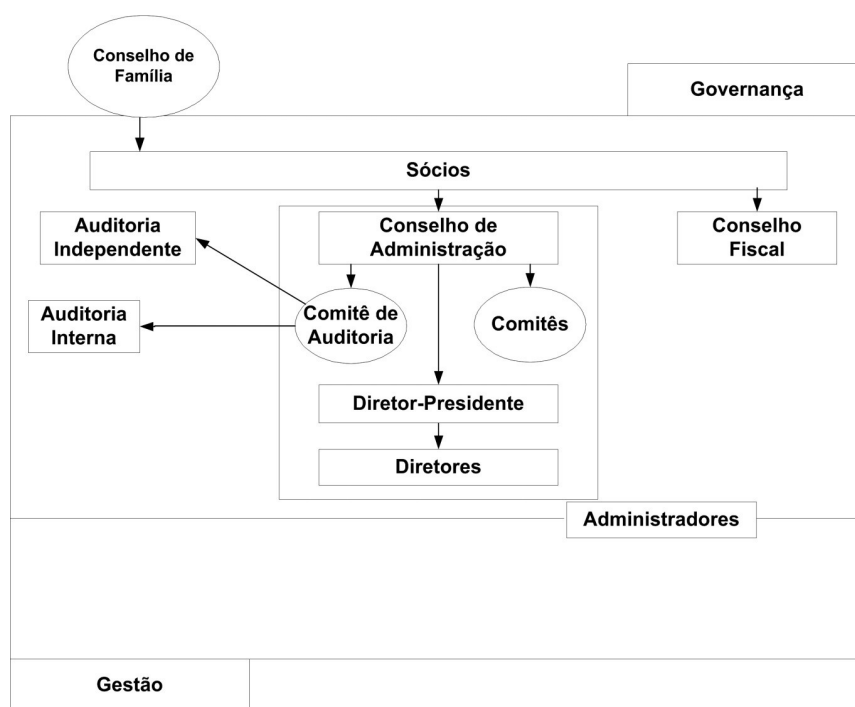
Figura 2.1 – Sistema de Governança Corporativa
Adaptado de IBGC (2009)

Para garantir que os princípios da Governança Corporativa sejam efetivos, seja por sua vontade expressa ou requerida face ao ambiente regulatório em que se encontra, as organizações lançam mão de modelos de controle interno e gestão de risco.

O principal modelo norteador da estruturação de sistemas de controles internos e de gestão de risco é o COSO – *The Committee of Sponsoring Organizations of the Treadway Commission* (Comitê das Organizações Patrocinadoras).

O COSO é uma entidade sem fins lucrativos dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa, que foi criada por iniciativa do setor privado para estudar as causas de ocorrências de fraudes em relatórios financeiros e contábeis e desenvolver recomendações para empresas de capital aberto e para instituições de ensino.

Em 1992, o COSO publicou um trabalho intitulado *Internal Control – Integrated Framework* (Controle Interno – Um Modelo Integrado), que se tornou referência para as organizações do mundo todo para que elas estruturem seus sistemas de controle interno.

De acordo com o COSO, o controle interno é um processo efetuado pelo conselho de administração, executivos ou qualquer outro funcionário de uma organização, com a finalidade de possibilitar o máximo de garantia nas seguintes categorias de objetivos:

- ❒ **Eficiência e eficácia das operações:** salvaguarda de seus ativos e prevenção e detecção de fraudes e erros.
- ❒ **Confiabilidade das demonstrações financeiras:** exatidão, integridade e confiabilidade dos registros financeiros e contábeis.
- ❒ **Conformidade com as leis e regulamentos vigentes:** aderência às normas administrativas, às políticas da empresa e à legislação à qual está subordinada.

Em 2001, o COSO iniciou um projeto para a determinação de um modelo de Risco Corporativo, que resultou no documento intitulado *Enterprise Risk Management Framework*, ampliando o alcance dos controles internos e definindo processos para o gerenciamento de riscos corporativos.

A Figura 2.2 mostra como esses sistemas de controle e risco e de direitos decisórios da Governança Corporativa criam as restrições de operação dos

serviços e projetos de TI. Por exemplo, supondo que o sistema de controle de riscos aponta que é um risco não haver um método de gerenciamento de projetos de TI; a TI deve então implementar este método (controle interno), em relação ao qual o sistema de controle interno irá verificar a aderência periodicamente, ou seja, realizará uma auditoria para verificar se os projetos estão aplicando, de fato, o método.
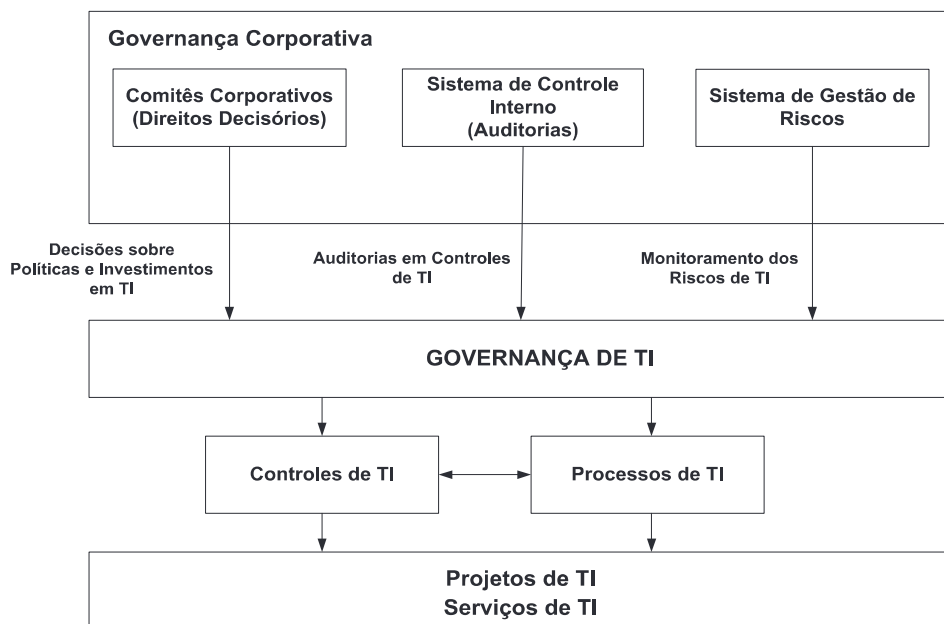
Figura 2.2 – Integração Governança Corporativa x Governança de TI

Nesse contexto, há dois regulamentos bastante fortes, que têm dado um grande poder de fogo às áreas de "controle interno" da maioria das organizações: o *Sarbanes-Oxley Act* e o Acordo da Basileia II.

O primeiro atinge empresas de capital aberto e que têm ações nas bolsas de valores norte-americanas. No Brasil, atinge algumas empresas de capital majoritariamente nacional e as subsidiárias de empresas transnacionais.

A segunda atinge instituições financeiras de uma forma geral. É uma regulamentação patrocinada pelo *Bank for International Settlements* ou BIS, que

seria o "Banco Central dos Bancos Centrais", com sede na cidade de Basileia, na Suíça. A partir dela, as autoridades bancárias principais de vários países criaram modelos derivados (no caso do Banco Central do Brasil, temos a Resolução 3380, também abordada neste capítulo).

Ambas as regulamentações têm forte impacto na área de TI e fazem parte do nosso modelo de Governança de TI, pois, dependendo da organização, devem ser contempladas pelo alinhamento estratégico. Seu atendimento se reveste de vários projetos constantes do portfólio de TI, que vão criar restrições às operações de serviços de TI.

Agora vamos explorar um pouco mais as implicações desses marcos de regulação externos.

2.2 Entendendo as implicações do *Sarbanes-Oxley Act*

2.2.1 O que é o *Sarbanes-Oxley Act* e qual a sua finalidade

Os motivadores do *Sarbanes-Oxley Act* (vide Sarbanes & Oxley 2002), como é conhecido no mundo dos negócios, foram os escândalos financeiros acontecidos em companhias abertas nos Estados Unidos como a Enron e outras, que minaram a confiança dos investidores no mercado de capital americano (em especial dos que investiam em ações dessas companhias nas bolsas de valores). Para quem não sabe, a bolsa de valores é o principal meio de investimento da maioria das famílias norte-americanas. Portanto, manter a credibilidade do "sistema" é vital para os legisladores americanos e para os responsáveis pela condução econômica dos Estados Unidos.

Os objetivos principais dessa lei são proteger os investidores do mercado de capitais americano de fraudes contábeis e financeiras de companhias abertas, assim como instituir uma série de penalidades contra crimes relacionados. Seu foco é sobre "controles internos sobre relatórios financeiros".

De acordo com Ramos (2004):

> *O termo "controle interno sobre relatórios financeiros" é definido como o processo projetado por, ou sob a supervisão do principal executivo e do principal responsável por finanças do emitente, ou pessoas que desempe-*

nham funções similares, efetivados pelo comitê de diretores do emitente, pela gerência ou outras pessoas, para prover garantia razoável relacionada à confiabilidade de emissão de relatórios financeiros e a preparação de relatórios de resultados financeiros para propósitos externos, de acordo com princípios de contabilidade geralmente aceitos – GAAP. Inclui política e procedimentos para:
(1) Manter registros que, em razoável detalhe, com exatidão e de forma correta, reflitam as transações e disposições dos ativos do emitente.
(2) Prover garantia de que as transações sejam registradas quando necessário para permitir a preparação de declarações de resultados financeiros de acordo com princípios contábeis geralmente aceitos, e que as receitas e despesas do emitente sejam feitas somente de acordo com autorizações da gerência e diretores do emitente.
(3) Prover garantia relacionada à prevenção ou detecção, no momento preciso, de aquisições não autorizadas, uso ou disposição dos ativos do emitente que possam ter um efeito material nas declarações dos resultados financeiros.

O nome dessa lei federal americana, patrocinada pelos congressistas norte-americanos Sarbanes e Oxley e publicada em agosto de 2002 para regular as responsabilidades e práticas de auditoria em empresas abertas, é: *"Public Accounting Reform and Investor Protection Act".*

A *Stock Exchange Comission* – SEC (que vem a ser a equivalente à nossa Comissão de Valores Mobiliários – CVM), autoridade que regula o mercado de capitais norte-americano, tem a responsabilidade por estabelecer as regras para implantar o *Sarbanes-Oxley Act*. Tais regras incluem guias para a elaboração de relatórios financeiros pelos CEO (*Chief Executive Officer* – geralmente o presidente da empresa) e o CFO (*Chief Financial Officer* – responsável máximo pelas finanças de uma empresa).

Para definir regras para os auditores independentes a respeito da lei, foi criada no contexto da SEC o *Public Company Accounting Oversight Board*, que é uma organização não governamental dedicada a criar normas a partir da lei.

O SOX (*Sarbanes-Oxley Act*) é composto pelos seguintes títulos:

- Título I : *Public Company Accounting Oversight Board.* Trata do PCAOB, que é uma organização não governamental que deve regis-

trar as auditorias e estabelecer os padrões de auditoria relativos aos controles financeiros das empresas abertas.

- Título II: *Auditor Independence.* Estabelece que os auditores sejam independentes e que haja rotatividade entre empresas de auditoria.
- Título III: *Corporate Responsibility.* Atribui as responsabilidades corporativas, em termos da formação de um comitê de auditoria, da sua composição e dos requisitos sobre o envio de relatórios à SEC e outros tipos de conduta requeridos dos CEOs, CFOs e demais diretores.
- Título IV: *Enhanced Financial Disclosures.* Estabelece novas regras para a elaboração e publicação de resultados financeiros, assim como requer que a administração mantenha um sistema de controle interno adequado.
- Título V: *Analyst Conflicts of Interest.* Estabelece regras para que não haja conflitos de interesse na atuação de analistas de corretoras de valores ou de administração de fundos.
- Título VI: *Comission Resources and Authority.* Estabelece regras para autorização de fundos para a SEC, assim como a autoridade da SEC para suspender, temporariamente ou não, empresas e profissionais de auditoria.
- Título VII: *Studies and Reports.* Aqui o SOX autoriza a SEC a efetuar estudos e relatórios relativos à consolidação de firmas de auditoria, agências de "*rating*" de risco, violações profissionais no âmbito do mercado de capitais, análises dos resultados das ações da SEC e estudos de bancos de investimentos.
- Título VIII: *Corporate and Criminal Fraud Accountability.* Estabelece regras específicas e penalidades para a destruição de registros corporativos, assim como para alteração de dados e falsificações.
- Título IX: *White-Collar Crime Penalty Enhancements.* Contém penalidades para crimes do colarinho branco.
- Título X: *Corporate Tax Returns.* Estabelece que o CEO deve, obrigatoriamente, assinar o imposto de renda da pessoa jurídica.
- Título XI: *Corporate Fraud Accountability.* Define a responsabilidade corporativa pela comunicação de informações financeiras de resultados fraudulentos.

2.2.2 Requisitos do SOX que afetam a TI

Para a TI, as seções 302 e 404 do SOX são de especial importância.
A seção 302 especifica que:

- ❒ O CEO e o CFO devem revisar os relatórios financeiros.
- ❒ Com base no conhecimento do CEO e do CFO, os relatórios não contêm nenhuma declaração falsa de um fato material ou omissão, para fazer a declaração de resultados.
- ❒ Com base no conhecimento do CEO e do CFO, outras informações financeiras incluídas representam corretamente, em todos os aspectos materiais, a condição financeira, resultados de operações e fluxos de caixa nos períodos representados pelos relatórios.
- ❒ O CEO e o CFO são responsáveis por manter e estabelecer controles e procedimentos sobre a emissão de relatórios financeiros e controles internos sobre tais relatórios.
- ❒ Os sistemas de controle interno sobre a emissão de relatórios financeiros devem ser projetados sob a supervisão do CEO e do CFO, incluindo as subsidiárias.
- ❒ Os sistemas de controle internos sobre relatórios financeiros também devem ser projetados sob a supervisão do CEO e do CFO.
- ❒ Deve ser avaliada a efetividade do sistema de controle sobre a emissão de relatórios financeiros.
- ❒ Devem ser comunicadas mudanças nos controles internos sobre relatórios financeiros, considerando o último ano fiscal.
- ❒ Devem ser comunicadas as deficiências dos sistemas de controle interno que possam afetar a habilidade da empresa em registrar, processar, sumarizar e comunicar informações financeiras.
- ❒ Deve ser comunicada qualquer fraude que envolva a gerência ou outros empregados que tenham um papel significante nos registros do controle interno sobre relatórios financeiros.

A Seção 404, por sua vez, especifica que:

- ❒ A administração tem a responsabilidade de estabelecer e manter uma estrutura adequada de controle interno e procedimentos para relatórios financeiros.

- ❐ A administração deve avaliar a efetividade do sistema de controle interno sobre relatórios financeiros.
- ❐ Deve ser realizada uma auditoria externa específica sobre a avaliação interna da efetividade do sistema de controle interno feita pela administração.

Para atender aos requisitos do SOX, as informações financeiras sobre os resultados devem atender aos seguintes princípios:

- ❐ O conteúdo da informação deve ser apropriado.
- ❐ A informação deve estar disponível no momento em que for necessária.
- ❐ A informação é atual ou pelo menos a última disponível.
- ❐ Os dados e as informações estão corretas.
- ❐ A informação é acessível aos usuários interessados.
- ❐ Há um sistema de controle interno sobre relatórios financeiros que garante todos os demais itens anteriores.

Esses requisitos afetam a TI de forma bastante significativa. Lembramos que as informações financeiras e de resultados são oriundas de todos os processos de negócio que geram fatos contábeis e financeiros para a empresa, e que podem estar automatizados ou não.

Portanto, praticamente todos os sistemas transacionais de uma empresa relativos a pagamento de pessoal, pagamento de benefícios a pessoal, transações com fornecedores (compras, aplicação de recursos financeiros) e clientes (vendas, captação de recursos financeiros), com acionistas, com o governo, gestão de recursos financeiros etc. devem ser considerados quando pensamos no SOX.

No contexto de um sistema de controle interno, os riscos são identificados e mitigados, os controles são estabelecidos e executados, os registros e sistemas de controle são desenvolvidos e mantidos e toda a sistemática é monitorada.

A TI, como sabemos, é um elemento crítico como fonte de risco para a continuidade do negócio e para o atendimento ao SOX.

A Tabela 2.1 mostra as principais implicações operacionais do SOX para a TI, considerando os processos de TI (vide em capítulos posteriores as considerações dos modelos de melhores práticas de TI):

Requisitos de qualidade da informação	Implicações do SOX
O conteúdo da informação deve ser apropriado.	• Processo de desenvolvimento de requisitos de software. • Processo de gerenciamento de requisitos de software. • Métodos de engenharia de software. • Processos de verificação (teste). • Processos de validação (aceitação pelos usuários). • Processos de segurança da informação empregados nos aplicativos. • Processos de aceitação de produtos de terceiros. • Processo de gestão da mudança e da configuração.
A informação deve estar disponível no momento em que for necessária.	• Disponibilidade de aplicativos. • Disponibilidade da infraestrutura. • Gerenciamento de incidentes e problemas no ambiente de produção. • Suporte aos usuários. • Gestão de aplicativos e de ativos de TI. • Processos de gerenciamento da infraestrutura. • Segurança da infraestrutura. • Gerenciamento da contingência. • Gerenciamento de disponibilidade e desempenho.
A informação é atual ou pelo menos é a última disponível.	• Processos de gerenciamento de dados. • Planejamento e gerenciamento da contingência e de desastres. • Segurança da informação na infraestrutura.
Os dados e as informações estão corretas.	• Segurança da informação em aplicativos. • Segurança da infraestrutura de TI. • Teste de software. • Controle da mudança e da configuração. • Gerenciamento de dados. • Gerenciamento de requisitos.
A informação é acessível aos usuários interessados.	• Segurança da informação referente a controle de acessos e privilégios. • Controle de autorizações.
Há um sistema de controle interno sobre relatórios financeiros.	• Avaliação de riscos de TI. • Gestão da qualidade. • Planos de desastres e recuperação.

Tabela 2.1 – Implicações do SOX para TI

2.2.3 Impacto do SOX na Governança de TI

O SOX impacta a Governança de TI no que diz respeito aos seguintes aspectos:

❒ As questões relativas ao SOX devem ser tratadas no Plano de Tecnologia da Informação.

- ❒ Novos controles (funcionalidades) em aplicações do legado devem ser implantados.
- ❒ Novas aplicações devem ser implantadas.
- ❒ Processos de TI existentes devem ser ajustados e melhorados para mitigar riscos.
- ❒ Novos processos de TI devem ser projetados e implantados.
- ❒ Ocorrência de prováveis mudanças na estrutura organizacional de TI em função dos processos ajustados e também dos novos.
- ❒ Novos indicadores de desempenho deverão ser definidos e implantados.
- ❒ Os riscos de TI devem ser monitorados constantemente.

Finalizando este tema, o CIO deve ser peça fundamental no esforço da empresa para se ajustar ao SOX, devendo participar ativamente do projeto de adequação.

2.3 Entendendo as implicações do Acordo da Basileia II

2.3.1 O que é o Acordo da Basileia II

Estabelecido pelo *Bank for International Settlements*, BIS, sediado na cidade suíça da Basileia (que vem a ser o "Banco Central dos Bancos Centrais"), o Acordo da Basileia II (vide BIS 2001) estipula requisitos de capital mínimo para as instituições financeiras, em função dos seus riscos de crédito e operacionais. O acordo possui três pilares:

- ❒ O primeiro pilar estabelece regras e procedimentos para cálculo dos requisitos de capital, tendo em vista os riscos de crédito e operacionais, de acordo com a aplicação de abordagens distintas de avaliação e mitigação de riscos. Risco de crédito é a perda econômica sofrida pela incapacidade voluntária ou involuntária do tomador do crédito em atender às suas obrigações contratuais no tempo requerido. No caso dos bancos, a metodologia deve atender tanto a uma transação individual de crédito como a uma carteira de crédito, ou seja, o portfólio de crédito da instituição. Risco operacional, por sua vez, é o risco de

perdas financeiras diretas ou indiretas resultantes de processos internos inadequados, de falhas nos processos, pessoas e sistemas, ou mesmo de eventos externos.

- O segundo pilar estabelece regras para que os Bancos Centrais de cada país executem auditorias nas instituições financeiras, visando avaliar a aplicação dos métodos de gestão de risco e a avaliação e mitigação de riscos de crédito e operacionais, assim como a emissão de informações para o mercado acerca da exposição do risco da instituição.
- O terceiro pilar estabelece regras para a comunicação para o mercado, dos requisitos mínimos de capital, face aos riscos e aos métodos e resultados de avaliações de riscos, conforme estabelecido pelo primeiro pilar.

2.3.2 Implicações do Acordo da Basileia II sobre a TI

Atualmente o Banco Central do Brasil vem auditando as áreas de TI dos bancos através do instrumento denominado CobiT, desenvolvido pela *Information Systems Audit and Control Association* – ISACA (este *framework* é apresentado mais adiante).

Como os bancos no Brasil estão em estágio extremamente avançado no que diz respeito à integração, uso de tecnologias, diversidade de canais e diversidade de produtos, a questão "risco operacional" de TI é primordial. A TI é um dos principais elementos do risco operacional de um banco, juntamente com pessoas e processos de negócio.

No que tange ao risco operacional, o impacto do Acordo da Basileia abrange praticamente todo o espectro de processos de TI e respectivas áreas organizacionais.

Do ponto de vista do risco de crédito, o impacto recai sobre:

- Capacidade de armazenamento de dados em face da granularidade de informações requeridas de cada cliente, visando avaliar riscos de forma mais consistente.
- Integridade das informações acerca das transações do banco.
- Integridade das informações armazenadas sobre os clientes e operações de crédito.
- Segurança dessas informações.
- Contingências na operação.
- Planejamento de capacidade.

- ❒ Planejamento de desastre e recuperação.
- ❒ Integridade do processo de emissão de relatórios requeridos pelo BIS.

Analogamente ao que falamos no caso do SOX, relativamente ao Acordo da Basileia, o CIO ou equivalente deve:

- ❒ Inserir as questões do acordo em seu Plano de Tecnologia da Informação.
- ❒ Implantar novos processos de TI.
- ❒ Ajustar ou melhorar processos existentes.
- ❒ Ajustar a estrutura organizacional de TI para acomodar novos processos.
- ❒ Definir e implantar novos indicadores de desempenho, caso seja necessário.
- ❒ Tratar a gestão de riscos (planejamento e monitoramento) de TI como seu processo com identidade própria na organização de TI.

2.4 O impacto da Resolução 3380 do Banco Central do Brasil

Em junho de 2006 foi publicada a Resolução 3380 do Banco Central do Brasil, que determina que as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central implementem sua própria estrutura de gerenciamento de risco.

Conforme definição na resolução, risco operacional é a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. No que tange à tecnologia da informação, a resolução refere-se a falhas em sistemas como risco operacional. Alguns riscos apontados, tais como interrupção de atividades da instituição e danos a ativos, também podem ser originados pela tecnologia da informação.

De acordo com a resolução, deve-se identificar, avaliar, monitorar, controlar e mitigar os riscos da instituição:

- ❒ Os riscos operacionais devem ser identificados, avaliados, monitorados, controlados e mitigados (essa gestão deve ser permanentemente executada).

- ❒ Planos de continuidade de negócios devem ser elaborados, testados e atualizados.
- ❒ Os riscos dos fornecedores de serviços devem ser gerenciados.

O ponto de partida utilizado pela maioria das instituições é a avaliação dos riscos de TI com base nos processos do CobiT (leia no capítulo 6 maiores detalhes sobre este modelo).

Outra abordagem é a elaboração de mapas de riscos por negócio, onde os riscos que a TI oferece para o negócio são identificados, avaliados, monitorados, controlados e mitigados. Um exemplo de risco em um processo de *internet banking* é a disponibilidade das aplicações; o mesmo ocorre para uma transferência eletrônica de fundos. Dependendo da criticidade do risco para o negócio, é determinada a frequência para a ocorrência das auditorias sobre TI.

Nesse contexto, quem realiza a gestão de riscos é uma área de gestão de riscos corporativos, cujas informações devem ser tratadas pela TI para projetar e implementar ações de mitigação (controles internos de TI).

Por exemplo, em processos críticos de negócios, geralmente são elaborados Planos de Continuidade do Negócio, que irão resultar na elaboração de Planos de Desastre e Recuperação pela TI, visando recuperar serviços de TI que apoiam o processo de negócio.

O mais importante é que tanto o sistema de controle interno como o de risco são grandes aliados na implantação da Governança de TI na organização.